Phishing+Telegram: Solicitação de reembolso da Autoridade Tributária?

seguranca-informatica.pt/phishingtelegram-solicitacao-de-reembolso-da-autoridade-tributaria/

August 31, 2021

Phishing+Telegram: Solicitação de reembolso da Autoridade Tributária?
Se nos últimos dias recebeu um email em nome da Autoridade Tributária e Aduaneira para a solicitação de um reembolso, cuidado, porque pode/**deve ser fraude.**

Para começar, não vamos sequer debater questões relacionadas com certificado digital. Vale o que vale o cadeado hoje em dia. Em detalhe, a campanha tem sido disseminada pelos malfeitores através do seu veículo favorito, o email. Em destaque pode ser encontrada uma mensagem na *landing-page* maliciosa que tenta, de certa forma, iludir a vítima a introduzir os seus dados: "**Para evitar atrasos, certifique-se de enviar este formulário antes do prazo …**".

Ao longo dessa página são solicitados os seguintes dados pessoais:

- **NIF**
- **E-mail**
- **Telefone**
- **Número do cartão de crédito / Data / Código de Segurança + 3D secure code**

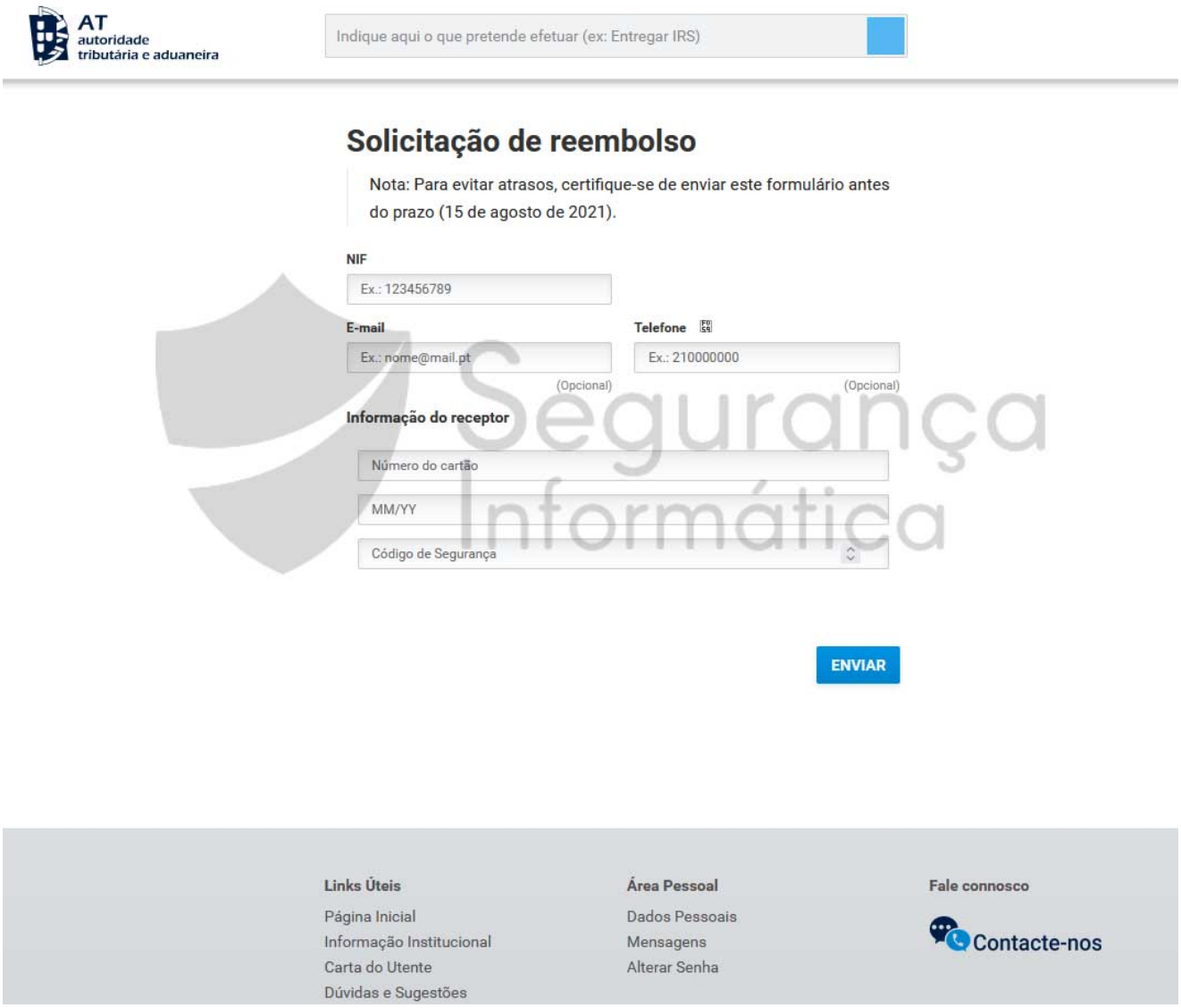


Figura 1: *Landing-page inicial da campanha solicitando detalhes da vítima.*

Ao analisar o código fonte da página inicial apresentada na Figura 1, é possível identificar um conjunto de validações aos detalhes introduzidos pela vítima. Esse trecho de código foi desenvolvido em JavaScript como ilustrado na Figura 2.

Figura 2: *Código JavaScript responsável por validar o input de dados da vítima, incluindo detalhes do cartão de crédito.*

Ao prosseguir com o esquema malicioso, a vítima é conduzida até à página "**/pt/pago/submit.php**" responsável por recolher e tratar os detalhes introduzidos no formulário inicial. A resposta do servidor é um código HTTP-302, um redireccionamento para a página no caminho: "**/pt/pago/SIBS.php**".

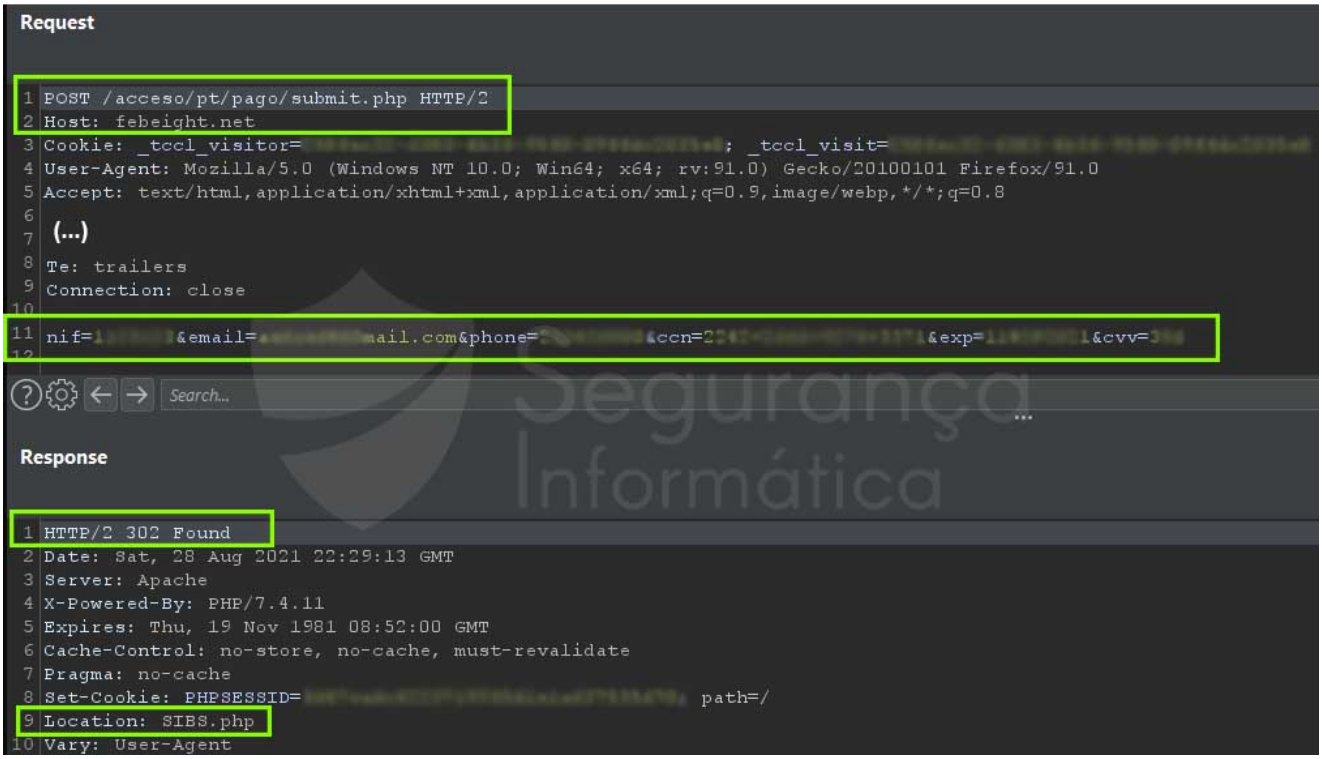


Figure 3: *HTTP-302 para outra página alvo solicitando código 3D secure para autenticação como meio de garantir legitimidade e autenticidade no acesso.*

Ao cair na última página da campanha "**SIBS.php**", é aprentado o formulário para introdução do código de autenticação 3D secure – uma farsa!

Figura 4: *Formulário solicitando o código 3-D SECURE.*

O 3D Secure é um protocolo de segurança que tem como objetivo garantir a proteção e a confiança nos meios de pagamento eletrónicos, permitindo a autenticação do titular do cartão e a confirmação de que o pagamento está a ser feito por ele.
Não introduza neste formulário os seu código, porque certamente não será cobrado um montante de 0.01 pelos criminosos.

O melhor amigo – Telegram

Como já observado em outras campanhas de phishing desta linha e também em vagas de malware, os criminosos utilizam as funcionalidades e segurança da API do Telegram para transferir os dados das vítimas para um grupo/bot do Telegram. A partir daí prosseguem com a atividade maliciosa.

Após a introdução do código 3D de segurança, os detalhes são enviados para o grupo do Telegram na página PHP "**/acceso/pt/pago/submitsms.php**".

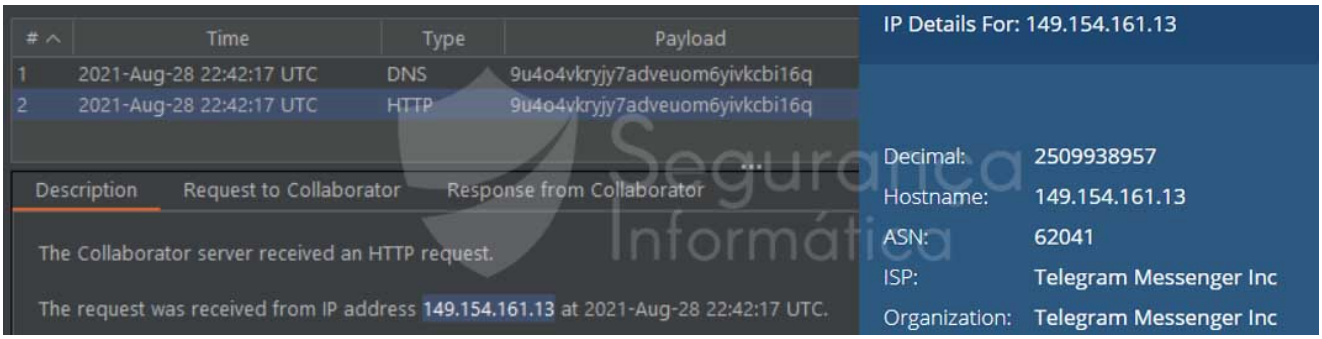


Figura 5: *Detalhes associados ao servidor Telegram extraídos da campanha.*

O Telegram é uma ferramenta bastante valiosa e tornou-se uma peça chave agora presente arsenal dos cribercriminosos. Numa campanha de malware afetando um banco também operando em Portugal, foi identificado um *modus operandi* semelhante ao que descrevemos anteriormente.

Nesse caso, os malfeitores abusavam da API do Telegram para enviar os detalhes das máquinas infetadas durante a kill-chain envolvendo o comprimetimento de computadores.

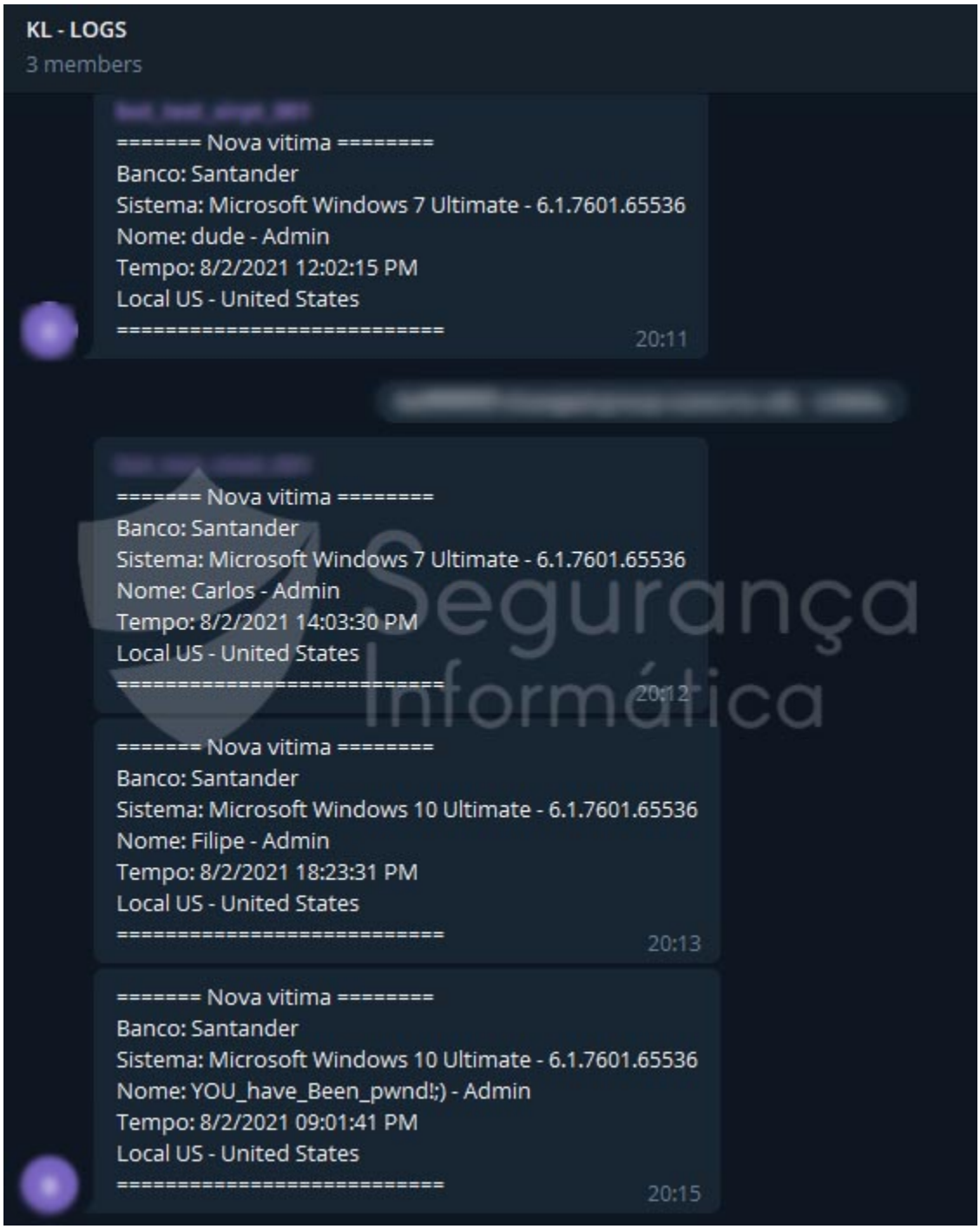
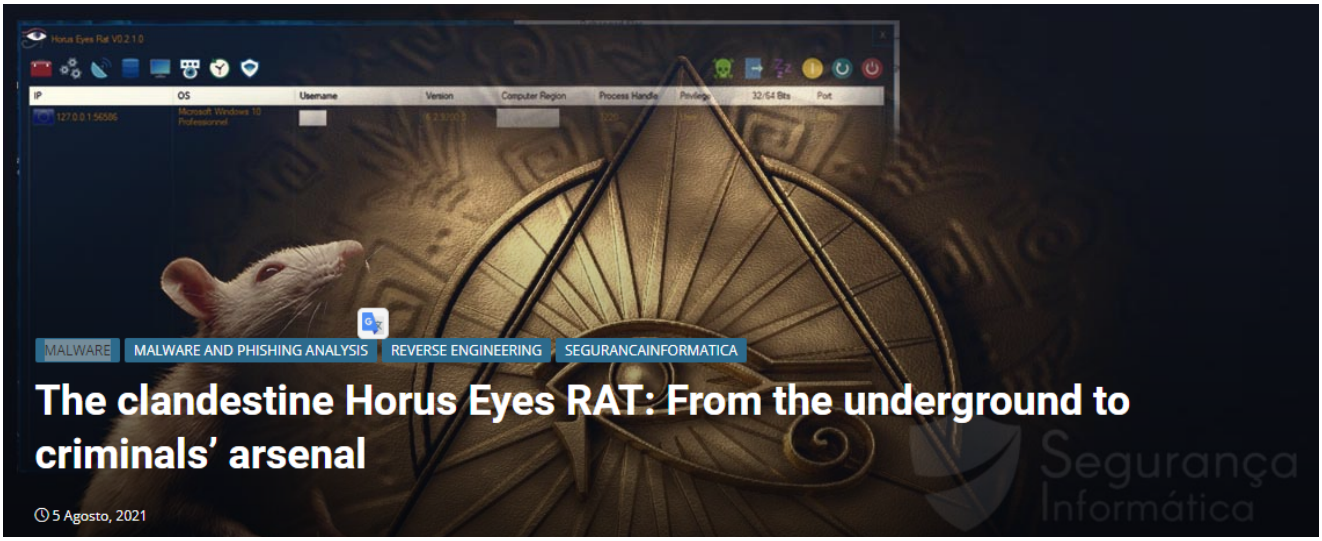


Figura 6: *Imagem do canal/grupo do Telegram com os detalhes dos computadores comprometidos pelo Horus Eyes RAT.*

Para mais detalhes sobre essa investigação:



Aos utilizadores sugere-se uma vez mais, alguma sensibilidade e análise quando confrontados com situações desta natureza.

Todos os endereços foram adicionados ao ***0xSI_f33d*** para que as organizações possam proceder ao bloqueio dos endereços de IP/domínios de forma eficaz.

Em caso de suspeita de campanhas de phishing ou malware partilhe a situação com as autoridades ou através do **formulário disponível aqui**, ou submeta a URL maliciosa/suspeita para o **0xSI_f33d.**

Indicadores de Compromisso (IOCs)

```
https://febeight.]net/acceso/pt/
```

Sumissões no 0xSI_f33d

https://feed.seguranca-informatica.pt/0xsi_f33d_id.php?id=2887

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources

Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.